



# **Handbuch Desktop Management**

hp Workstation xw4000

hp Workstation xw6000

Dokument-Teilenummer: 301201-041

**Oktober 2002**

Dieses Handbuch enthält Definitionen und Anleitungen zur Verwendung der Funktionen für Sicherheit und der Intelligent Manageability, die bei bestimmten Modellen voreingestellt sind.

© 2002 Hewlett Packard Company

Compaq, das Compaq Logo, ROMPaq und iPAQ sind Marken der Compaq Information Technologies Group, L.P. in den USA und/oder anderen Ländern.

Microsoft, MS-DOS, Windows und Windows NT sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Intel, Pentium, Intel Inside und Celeron sind Marken der Intel Corporation in den USA und/oder anderen Ländern.

Alle anderen in diesem Handbuch verwendeten Produktnamen können Marken der jeweiligen Unternehmen sein.

Die Hewlett-Packard Company haftet nicht für technische oder redaktionelle Fehler und Mängel in diesem Dokument. Ferner übernimmt die Hewlett-Packard Company keine Haftung für Schäden, die direkt oder indirekt auf Lieferung, Leistung und Nutzung dieses Materials zurückzuführen sind. Die Informationen in diesem Dokument werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt und können ohne vorherige Ankündigung geändert werden. Darüber hinaus werden keine Gewährleistungen übernommen, einschließlich, aber nicht beschränkt auf, ausdrückliche oder konkludente Gewährleistungen für die Tauglichkeit und Eignung für einen bestimmten Zweck. Die Garantien für HP Produkte werden ausschließlich in der entsprechenden, zum Produkt gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten.

Dieses Dokument enthält Informationen, die durch das Urheberrecht geschützt sind. Ohne schriftliche Genehmigung der Hewlett-Packard Company darf dieses Dokument weder kopiert noch in anderer Form vervielfältigt oder übersetzt werden.



**VORSICHT:** In dieser Form hervorgehobener Text weist darauf hin, dass die Nichtbeachtung zu Verletzungen oder zum Tod führen kann.

---



**ACHTUNG:** In dieser Form hervorgehobener Text weist darauf hin, dass die Nichtbeachtung zu Beschädigungen der Geräte oder zum Verlust von Daten führen kann.

---

Handbuch Desktop Management  
hp Workstation xw4000  
hp Workstation xw6000  
Erste Ausgabe (Oktober 2002)  
Dokument-Teilenummer: 301201-041

---

# Inhalt

## **Handbuch Desktop Management**

Erste Konfiguration und erster Einsatz .....	2
Remote System Installation .....	3
Software-Aktualisierung und -Management .....	3
Altiris eXpress .....	4
Altiris eXpress PC Transplant Pro .....	6
Altiris eXpress HP/Compaq Client Manager .....	6
System Software Manager .....	7
Benachrichtigung über Produktänderungen .....	7
ActiveUpdate .....	8
ROM-Flash .....	8
Remote-ROM-Flash .....	9
FailSafe-Boot-Block-ROM .....	9
Replizieren des Setup .....	12
Dual-State-Netzschalter .....	13
Power Management .....	14
World Wide Website .....	15
Bausteine und Partner .....	15
Desktop Management Interface (DMI) .....	16
Wired for Management .....	16
Bestandsüberwachung und Sicherheit .....	17
Kennwort-Schutz .....	21
Löschen des Kennworts für den Systemstart oder des Setup-Kennworts .....	25
Network Server Mode (Netzwerk-Server-Modus) .....	27
DriveLock .....	28
Smart Cover Sensor .....	31
Smart Cover Lock .....	32
Master Boot Record Security (Master Boot Record-Sicherheit) .....	35
Diebstahlsicherung .....	38
Fingerprint Identification Technology .....	38

Fehlermeldung und Fehlerbehebung . . . . .	39
Drive Protection System . . . . .	39
Ultra ATA Integritäts-Überwachung . . . . .	39
Überspannungstolerantes Netzteil . . . . .	40
Thermosensor . . . . .	40

## **Index**

---

# **Handbuch Desktop Management**

HP war 1995 mit der Einführung der ersten vollständig verwaltbaren Desktop-PCs ein Vorreiter im Bereich der Desktop Manageability. Seither ist HP führend bei der angestrebten Entwicklung der Normen und der Infrastruktur, die zum effektiven Einsatz, Management und zur Konfiguration von Desktops, Workstations und Notebooks erforderlich sind. HP Intelligent Manageability bietet standardisierte Lösungen zur Verwaltung und Steuerung von Desktops, Workstations und Notebooks in einer Netzwerkumgebung. HP arbeitet eng mit marktführenden Anbietern von Management-Software-Lösungen zusammen, um die Kompatibilität zwischen Intelligent Manageability und diesen Produkten sicherzustellen. Intelligent Manageability ist ein wichtiger Aspekt des umfassenden Engagements von HP, Ihnen PC Lifecycle-Lösungen zu bieten, die Sie während der vier Phasen des Lebenszyklus eines Desktop-PCs unterstützen – von der Planung und dem Einsatz über die Verwaltung bis zur Umstellung.

Dieses Handbuch fasst die Möglichkeiten und Funktionen der sieben Hauptkomponenten des Desktop Managements zusammen.

- Erste Konfiguration und erster Einsatz
- Remote System Installation
- Software-Aktualisierung und -Management
- ROM-Flash
- Bausteine und Partner
- Bestandsüberwachung und Sicherheit
- Fehlermeldung und Fehlerbeseitigung



Die Unterstützung spezieller, in diesem Handbuch beschriebener Funktionen kann sich je nach Modell oder Software-Version unterscheiden.

---

## Erste Konfiguration und erster Einsatz

Die Computer werden mit vorinstalliertem Systemsoftware-Image geliefert. Nach einem kurzen Vorgang des „Auspakens“ der Software ist der Computer einsatzbereit.

Möglicherweise ziehen Sie es vor, das vorinstallierte Software-Image durch eine benutzerdefinierte System- und Anwendungssoftware zu ersetzen. Es gibt mehrere Methoden zum Ersetzen eines benutzerdefinierten Software-Images. Folgende Methoden können verwendet werden:

- Installation zusätzlicher Software-Anwendungen nach dem Auspacken des vorinstallierten Software-Images
- Verwendung von Software-Einsatz-Tools, wie etwa Altiris eXpress, Microsoft MS Batch oder Microsoft NT Distribution Share (NTDS), um die vorinstallierte Software durch ein benutzerdefiniertes Software-Image zu ersetzen.
- Verwendung eines Disk-Kopievorgangs zum Kopieren des Inhalts einer Festplatte auf eine andere

Die besten Einsatzverfahren hängen von Ihrer IT-Umgebung und den damit verbundenen Prozessen ab. Der Abschnitt zum PC-Einsatz auf der Website zu Lösungen und Dienstleistungen (<http://www.compaq.com/solutions/pcsolns>) bietet Ihnen Informationen zur Auswahl des besten Verfahrens. Hier finden Sie auch Handbücher und Dienstprogramme zur Integration von Einsatz-Tools auf Microsoft- oder PXE-Grundlage.

Die *Compaq Restore CD* (oder *Restore Plus! CD*), das ROM-basierte Setup und die Hardware mit ACPI-Unterstützung bieten zusätzliche Hilfe bei der Wiederherstellung der Systemsoftware, dem Konfigurations-Management, der Fehlerbeseitigung sowie bei der Energieverwaltung.

## Remote System Installation

Remote System Installation erlaubt Ihnen, Ihr System mit Hilfe der Software und der Konfigurationsinformationen von einem Netzwerk-Server zu starten und zu installieren. Remote System Installation wird normalerweise als Tool zur Systemeinrichtung und -konfiguration verwendet und kann darüber hinaus für die folgenden Aufgaben eingesetzt werden:

- Einsetzen eines Software-Images auf einem oder mehreren neuen PCs
- Formatierung eines Festplattenlaufwerks
- Installieren von Anwendungssoftware oder Treibern
- Aktualisieren des Betriebssystems, der Anwendungssoftware oder der Treiber

Drücken Sie die Taste **F12**, um Remote System Installation zu starten, wenn die Meldung *F12 = Network Service Boot* (Starten über Netzwerk) in der unteren rechten Ecke der HP Logoanzeige erscheint. Folgen Sie den Anleitungen auf dem Bildschirm, um fortzufahren.

HP und Altiris, Inc. haben sich zusammengeschlossen, um Tools zur Verfügung zu stellen, die den Einsatz und das Management von Firmen-PCs vereinfachen, weniger zeitaufwendig gestalten, die Total Cost of Ownership senken und die HP PCs zu den Client PCs mit der besten Manageability in Unternehmensumgebungen machen.

## Software-Aktualisierung und -Management

HP bietet verschiedene Tools für Software-Aktualisierung und -Management auf Desktop-Computern und Workstations:  
Altiris eXpress, Altiris eXpress PC Transplant Pro, Altiris eXpress HP/Compaq Client Manager, System Software Manager, Product Change Notification und ActiveUpdate.

## **Altiris eXpress**

HP und Altiris haben ihre Partnerschaft ausgebaut, um branchenführende Lösungen anbieten zu können, die die Verwaltung der Hardware und Software für Desktop-Computer, Notebooks, Handheld-Geräte und Server während des gesamten Lebenszyklus dieser Geräte vereinfachen. Altiris eXpress ermöglicht dem Systemadministrator die Erstellung und den schnellen Einsatz eines nach dem Firmenstandard benutzerdefinierten Software-Images auf einem oder mehreren vernetzten Client-PCs mit einer Schnittstelle, die so einfach zu verwenden ist wie der Windows Explorer. Altiris eXpress unterstützt Wired for Management von Intel und Preboot Execution Environment (PXE). Bei Verwendung der Funktionen von Altiris eXpress und Remote System Installation auf dem HP Computer ist es für den Systemadministrator nicht erforderlich, das Software-Image auf jedem neuen PC einzeln zu implementieren.

Die Altiris eXpress Lösungen bieten eine effiziente und effektive Methode, bestehende Prozesse zu automatisieren und Problembereiche in der IT-Umgebung anzugehen. Die Web-basierte Infrastruktur von Altiris eXpress verschafft Ihnen die Flexibilität, Ihre Systeme zu jeder Zeit und von jedem Ort aus zu verwalten – sogar von Ihrem iPAQ Pocket PC aus!

Die Altiris eXpress Lösungen sind modular und erweiterbar, so dass sowohl die Anforderungen von Arbeitsgruppen als auch die des gesamten Unternehmens erfüllt werden. Diese Lösungen können mit Client-Management-Tools anderer Anbieter integriert werden und bieten Erweiterungen für Microsoft BackOffice/SMS.

Die erweiterten Altiris eXpress Lösungen konzentrieren sich auf vier zentrale IT-Bereiche:

- Einsatz und Migration
- Software und Operations Management
- Bestandsverwaltung
- Help Desk und Problemlösung

Nach wenigen Minuten der Installation ist Altiris eXpress bereits in der Lage, ein Disketten-Image mit dem Betriebssystem, der Anwendungssoftware und dem Altiris eXpress Client zu installieren, ohne dass eine separate Startdiskette verwendet werden muss. Mit Altiris eXpress kann der Netzwerkadministrator folgende Aufgaben durchführen:

- Erstellen eines neuen oder Bearbeiten eines bereits vorhandenen Images oder Cloning eines PCs im Netzwerk, der möglicherweise das ideale Image enthält.
- Erstellen einer beliebigen Anzahl von benutzerdefinierten Disketten-Images für eine Vielzahl von Arbeitsgruppen.
- Bearbeiten von Image-Dateien durch Änderungen ohne Erstellen neuer Dateien. Dies ist möglich, da mit Altiris eXpress die Dateien in ihrem ursprünglichen Format gespeichert werden, also als NTFS-, FAT16- oder FAT32-Dateien.
- Einrichten eines „Neuen PC-Ereignisses“ – ein Skript, das automatisch ausgeführt wird, wenn ein neuer PC dem Netzwerk hinzugefügt wird. Mit dem Skript kann beispielsweise das Festplattenlaufwerk eines PC formatiert, ein Flash für ROM-BIOS durchgeführt und ein vollständiges Standardsoftware-Image installiert werden.
- Festlegen des Zeitplans für ein Ereignis, das für eine Gruppe von Computern ausgeführt werden soll.

Altiris eXpress bietet auch benutzerfreundliche Software-Verteilungsmöglichkeiten. Altiris eXpress kann zur Aktualisierung von Betriebssystemen und Anwendungssoftware von einer zentralen Konsole aus verwendet werden. Wenn Altiris eXpress in Verbindung mit System Software Manager verwendet wird, können auch ROM-BIOS und Gerätetreiber aktualisiert werden.

Weitere Informationen finden Sie unter  
<http://www.compaq.com/easydeploy>.

## **Altiris eXpress PC Transplant Pro**

Altiris eXpress PC Transplant Pro ermöglicht eine problemlose PC-Migration, indem alte Einstellungen, Voreinstellungen und Daten erhalten bleiben und auf schnelle und einfache Weise in die neue Umgebung überstellt werden. Anstelle von Stunden oder sogar Tagen dauert dieser Vorgang nur wenige Minuten, und schon können Sie mit Ihrem Desktop-Computer und den Anwendungen in gewohnter Weise arbeiten.

Weitere Informationen und Einzelheiten zum Herunterladen einer voll funktionsfähigen 30-Tage-Testversion finden Sie unter  
<http://www.compaq.com/easydeploy>.

## **Altiris eXpress HP/Compaq Client Manager**

Der Altiris eXpress HP/Compaq Client Manager integriert die HP Intelligent Manageability-Technologie innerhalb von Altiris eXpress und bietet so erstklassige Hardware-Management-Funktionen für HP Zugangsgeräte, wie z. B.:

- Ausführliche Anzeigen des Hardware-Inventars für die Bestandsverwaltung
- Überwachung des PC-Zustands und Diagnose
- Proaktive Benachrichtigung über Änderungen in der Hardware-Umgebung
- Über das Web zugängliche Berichtserstellung von wichtigen Detailinformationen, wie beispielsweise Warnmeldungen bei Gerätüberhitzung, mangelndem Speicherplatz usw.
- Remote-Aktualisierung von Systemsoftware, wie beispielsweise Gerätetreiber und ROM BIOS

Weitere Informationen zum Altiris eXpress HP/Compaq Client Manager finden Sie unter  
<http://www.compaq.com/easydeploy>.

## System Software Manager

System Software Manager (SSM) ist ein Dienstprogramm, mit dem Software auf Systemebene auf mehreren Systemen gleichzeitig aktualisiert werden kann. Wenn SSM auf einem PC-Client-System ausgeführt wird, erkennt es sowohl Hardware- als auch Software-Versionen und aktualisiert die betreffende Software dann von einem zentralen Repository aus, das auch als Dateispeicher bezeichnet wird. Treiberversionen, die von SSM unterstützt werden, sind auf der Website zum Herunterladen von Treibern sowie auf der Support Software CD durch ein spezielles Symbol gekennzeichnet. Besuchen Sie zum Herunterladen des Dienstprogramms oder zum Abrufen weiterer Informationen zu SSM die Website  
<http://www.compaq.com/im/ssmwp.html>.

## Benachrichtigung über Produktänderungen

PCN ist das HP Programm zur Benachrichtigung über Produktänderungen, mit dem in einer sicheren Website benutzerdefinierte Profile erstellt werden können, die proaktiv und automatisch Folgendes ermöglichen:

- Empfangen von E-Mail-Benachrichtigungen über Hardware- und Software-Änderungen für die meisten handelsüblichen Computer und Server.
- Empfangen von E-Mails mit *Customer Advisories* für die meisten handelsüblichen Computer und Server.

Die PCN-Website bietet außerdem die Möglichkeit zur Suche in allen Benachrichtigungen über Produktänderungen sowie in den *Customer Advisories* für die meisten handelsüblichen PCs und Server.

Weitere Informationen zu PCN und zum Erstellen eines benutzerdefinierten Profils finden Sie unter  
<http://www.compaq.com/pcn>.

## ActiveUpdate

ActiveUpdate ist eine Client-basierte Anwendung von HP. Der *ActiveUpdate* Client wird auf Ihrem lokalen System ausgeführt und verwendet Ihr benutzerdefiniertes Profil, um Software-Aktualisierungen für die meisten für Unternehmen geeignete Computer und Server von Compaq/HP proaktiv und automatisch herunterzuladen.

Weitere Informationen zu ActiveUpdate sowie zum Herunterladen der Anwendung und zum Erstellen eines benutzerdefinierten Profils finden Sie unter

<http://www.compaq.com/activeupdate>.

## ROM-Flash

Ihr Computer verfügt über einen programmierbaren Flash-ROM-Speicher (ROM=Read Only Memory, Nur-Lese-Speicher). Wenn Sie ein Setup-Kennwort in Computer Setup (F10) Utility einrichten, können Sie verhindern, dass der ROM-Speicher unbeabsichtigt aktualisiert oder überschrieben wird. Dies ist wichtig zur Gewährleistung des fehlerfreien Betriebs des Computers. Wenn Sie den ROM-Speicher aktualisieren müssen oder möchten, können Sie wie folgt vorgehen:

- Bestellen Sie eine aktualisierte *ROMPaq*™ Diskette von HP.
- Laden Sie die neuesten ROMPaq Images unter  
<http://www.compaq.com> herunter.



**ACHTUNG:** Für den maximalen Schutz des ROM-Speichers müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert die unbefugte Aktualisierung des ROM-Speichers. Mithilfe von System Software Manager kann der Systemadministrator das Setup-Kennwort auf mehreren PCs gleichzeitig einstellen. Weitere Informationen finden Sie unter  
<http://www.compaq.com/im/ssmwp.html>.

---

## Remote-ROM-Flash

Der Remote-ROM-Flash ermöglicht dem Systemadministrator, den ROM-Speicher von HP Computern direkt von der zentralen Netzwerk-Management-Konsole aus auf sichere Art und Weise remote zu aktualisieren. Da der Systemadministrator diese Aufgabe für mehrere Computer und PCs remote durchführen kann, ergibt sich dadurch ein konsistenter Einsatz und eine bessere Überwachung von HP PC ROM-Images über das Netzwerk. Dies führt außerdem zu höherer Produktivität und niedrigeren Total Cost of Ownership.



Der Computer muss eingeschaltet sein oder über die Remote Wakeup-Funktion eingeschaltet werden, um den Remote-ROM-Flash zu nutzen.

---

Weitere Details zu Remote-ROM-Flash finden Sie in den Informationen zu Altiris eXpress HP/Compaq Client Manager oder System Software Manager unter

<http://www.compaq.com/easydeploy>.

## FailSafe-Boot-Block-ROM

Der FailSafe-Boot-Block-ROM ermöglicht eine Wiederherstellung des Systems in dem unwahrscheinlichen Fall eines ROM-Flash-Ausfalls, z. B. bei einem Stromausfall während einer ROM-Aktualisierung. Der Boot-Block ist ein flash-geschützter Bereich des ROM-Speichers, der jedes Mal die Gültigkeit des ROM-Flash-Speichers überprüft, wenn der Computer eingeschaltet wird.

- Wenn der ROM-Speicher des Systems gültig ist, startet das System normal.
- Wenn der ROM-Speicher den Gültigkeitstest nicht besteht, bietet der FailSafe-Boot-Block-ROM ausreichend Unterstützung, damit das System von einer ROMPaq Diskette aus starten kann, die dem ROM-Speicher ein gültiges Image zuweist.

Wenn der Boot-Block einen ungültigen ROM-Speicher identifiziert, gibt das System eine Folge von akustischen Signalen aus (einmal lang und dreimal kurz), und die LED-Anzeige der Tastatur blinkt zweimal. Eine Meldung wird angezeigt, die angibt, dass das System in den Boot-Block-Wiederherstellungsmodus schaltet (modellabhängig).

Wenn Sie das System wiederherstellen möchten, nachdem es in den Boot-Block-Wiederherstellungsmodus geschaltet hat, führen Sie folgende Schritte aus:

1. Nehmen Sie alle Disketten aus den Laufwerken, und schalten Sie den Strom aus.
2. Legen Sie eine ROMPaq Diskette in das Diskettenlaufwerk ein.
3. Schalten Sie den Strom wieder ein.
4. Wenn keine ROMPaq Diskette gefunden wird, werden Sie aufgefordert, diese Diskette einzulegen und den Computer neu zu starten.
5. Wenn ein Setup-Kennwort eingerichtet wurde, leuchtet die LED-Anzeige der **Feststelltaste**, und Sie werden zur Eingabe des Kennworts aufgefordert.
6. Geben Sie das Setup-Kennwort ein.
7. Wenn das System erfolgreich von der Diskette startet und den ROM erfolgreich umprogrammiert, beginnen die drei LED-Anzeigen auf der Tastatur zu leuchten. Eine lauter werdende Abfolge von akustischen Signalen kennzeichnet zusätzlich den erfolgreichen Abschluss des Vorgangs.

So überprüfen Sie, ob der ROM-Flash erfolgreich war:

1. Legen Sie eine gültige ROMPaq Diskette in das Diskettenlaufwerk ein.
2. Unterbrechen Sie die Stromzufuhr zum System.
3. Schalten Sie die Stromversorgung wieder ein, um einen ROM-Flash durchzuführen.
4. Wenn der ROM-Flash erfolgreich ist, leuchten alle drei LED-Anzeigen auf der Tastatur auf, und eine Abfolge lauter werdender akustischer Signale ist zu hören.
5. Nehmen Sie die Diskette aus dem Laufwerk, und schalten Sie den Computer aus. Starten Sie anschließend den Computer neu.

Die folgende Tabelle gibt einen Überblick über die vom Boot-Block ROM verwendeten verschiedenen Kombinationen der LED-Anzeigen auf der Tastatur und ihre Bedeutungen sowie die Schritte in Verbindung mit diesen Kombinationen.

## Vom Boot-Block-ROM verwendete Kombinationen der LED-Anzeigen auf der Tastatur

<b>Modus Failsafe Boot Block</b>	<b>Farbe der LED-Anzeigen auf der Tastatur</b>	<b>Tastatur LED-Anzeigen</b>	<b>Zustand/Meldung</b>
Num-Funktion	Grün	Ein	ROMPaq Diskette nicht vorhanden oder fehlerhaft oder Laufwerk nicht bereit.*
Feststell-Funktion	Grün	Ein	Kennwort eingeben.*
Num, Feststelltaste, Rollen	Grün	Zweimal ein und aus (begleitet von einem langen und drei kurzen Tönen)	ROM-Flash fehlgeschlagen.*
Num, Feststelltaste, Rollen	Grün	Ein	Boot Block ROM-Flash erfolgreich. Schalten Sie den Strom aus und anschließend wieder ein, um neu zu starten.



Auf USB-Tastaturen blinken die Diagnoseanzeigen nicht.

## Replizieren des Setup

Dieses Verfahren ermöglicht es dem Systemadministrator, ohne großen Aufwand eine Setup-Konfiguration auf andere Computer des gleichen Modells zu kopieren. Auf diese Weise kann die Konfiguration mehrerer Computer schneller und mit größerer Konsistenz durchgeführt werden. So kopieren Sie das Setup:

1. Öffnen Sie das Menü der *Computer Setup Utilities (F10)*.
2. Klicken Sie auf **File** (Datei) > **Save to Diskette** (Speichern auf Diskette). Folgen Sie den Anleitungen auf dem Bildschirm.



Sie benötigen hierzu ein internes oder tragbares, externes Diskettenlaufwerk.

---

3. Um die Konfiguration zu replizieren, klicken Sie auf **File** (Datei) > **Restore from Diskette** (Wiederherstellen von Diskette), und folgen Sie den Anleitungen auf dem Bildschirm.

Altiris eXpress, System Software Manager und PC Transplant vereinfachen die Replikation der Konfiguration und benutzerdefinierten Einstellungen auf einem PC sowie das Kopieren dieser Daten auf einen oder mehrere andere PCs. Weitere Informationen finden Sie unter <http://www.compaq.com/easydeploy>.

## Dual-State-Netzschalter

Bei aktivierter ACPI-Funktion (Advanced Configuration and Power Interface) für Windows 98, Windows 2000, Windows Millennium und Windows XP übernimmt der Netzschalter entweder die Funktion des Ein-/Aus-Schalters oder der Standby-Taste. Im Standby-Modus wird die Stromzufuhr nicht komplett unterbrochen, sondern der Computer schaltet auf geringen Stromverbrauch um. Dadurch können Sie schnell in den Energiesparmodus schalten, ohne die Anwendungen schließen zu müssen, und Sie können ohne Datenverlust schnell in den gleichen Betriebszustand zurückkehren.

So ändern Sie die Konfiguration des Netzschalters:

1. Klicken Sie unter Windows 2000 mit der linken Maustaste auf die Schaltfläche **Start** und wählen Sie **Einstellungen > Systemsteuerung > Energieoptionen** aus.  
Klicken Sie unter Windows XP mit der linken Maustaste auf die Schaltfläche **Start** und wählen Sie **Systemsteuerung > Leistung und Wartung > Energieoptionen** aus.
2. Öffnen Sie unter **Eigenschaften von Energieoptionen** die Registerkarte **Erweitert**.
3. Wählen Sie im Abschnitt für die Netzschaltervorgänge die gewünschten Einstellungen für den Netzschalter aus.

Wenn Sie den Netzschalter als Standby-Taste konfiguriert haben, wird das System durch Drücken des Schalters auf sehr geringen Stromverbrauch (Standby-Modus) umgeschaltet. Wenn Sie erneut auf die Standby-Taste drücken, schalten Sie aus dem Standby-Modus auf Normalbetrieb um. Wenn Sie die Stromzufuhr ganz unterbrechen wollen, halten Sie den Netzschalter vier Sekunden lang gedrückt.

## Power Management

Power Management ist eine Energiesparfunktion, die einige Komponenten des Computers abschaltet, wenn diese nicht gebraucht werden. Dadurch kann Energie gespart werden, ohne dass der Computer ausgeschaltet werden muss.

Wenn ACPI (Advanced Configuration and Power Interface) für Windows 98, Windows 2000, Windows Millennium und Windows XP aktiviert wurde, können über das Betriebssystem Timeout-Werte (zulässiger Zeitraum der Inaktivität, bevor die Komponenten heruntergefahren werden) aktiviert, angepasst oder deaktiviert werden.

1. Klicken Sie unter Windows 2000 mit der linken Maustaste auf die Schaltfläche **Start** und wählen Sie **Einstellungen > Systemsteuerung > Energieoptionen** aus.

Klicken Sie unter Windows XP mit der linken Maustaste auf die Schaltfläche **Start** und wählen Sie **Systemsteuerung > Leistung und Wartung > Energieoptionen** aus.

2. Öffnen Sie unter **Eigenschaften von Energieoptionen** die Registerkarte **Energieschemas**.
3. Wählen Sie die gewünschten Einstellungen für die Energieschemas aus.

Verwenden Sie die Option **Eigenschaften von Anzeige**, um die Energiespareinstellungen für den Monitor festzulegen, zu ändern oder zu deaktivieren. Um die Option **Eigenschaften von Anzeige** aufzurufen, klicken mit der rechten Maustaste auf den **Windows-Desktop**, und wählen Sie **Eigenschaften** aus.

## **World Wide Website**

Die HP Techniker testen die von HP und Drittanbietern entwickelte Software nach strengen Richtlinien und entwickeln auf das jeweilige Betriebssystem zugeschnittene Support-Software, um eine optimale Leistung, Kompatibilität und Zuverlässigkeit von HP Computern zu gewährleisten.

Wenn Sie ein neues oder überarbeitetes Betriebssystem auf Ihrem Computer installieren, ist es wichtig, dass Sie auch die für das jeweilige Betriebssystem entwickelte Support-Software installieren. Wenn Sie mit einer Version von Microsoft Windows arbeiten möchten, die sich von der auf dem Computer vorinstallierten Version unterscheidet, müssen die entsprechenden Gerätetreiber und Dienstprogramme installiert werden, um sicherzustellen, dass alle Funktionen unterstützt werden und einwandfrei arbeiten.

HP hat das Auffinden, den Zugriff, die Bewertung und die Installation der neuesten Support-Software erheblich vereinfacht. Sie können die Software unter <http://www.compaq.com> herunterladen.

Die Website enthält die neuesten Gerätetreiber, Dienstprogramme und Flash-ROM-Images, die zur Ausführung des neuesten Microsoft Windows Betriebssystems auf Ihrem HP Computer erforderlich sind.

## **Bausteine und Partner**

Die Management-Lösungen von HP basieren auf verschiedenen Industriestandards, wie DMI 2.0, Web Based Enterprise Management, WfM (Wired for Management) von Intel, SNMP und PXE-Technologien (Preboot Execution Environment). Microsoft, Intel, Altiris und andere führende Unternehmen der Branche arbeiten eng mit HP zusammen, um ihre Verwaltungslösungen in HP Produkte zu integrieren und HP Kunden erstklassige Intelligent Manageability-Lösungen für PCs bereitzustellen. Weitere Informationen finden Sie unter <http://www.compaq.com/easydeploy>.

## Desktop Management Interface (DMI)

Die Desktop Management Task Force (DMTF) ist ein Branchenausschuss, der 1992 zur Standardisierung von Systems Manageability ins Leben gerufen wurde. Die DMTF legte die DMI (DMI = Desktop Management Interface)-Rahmenbedingungen für die Standardisierung des Zugangs zu PC-Konfigurationsdaten fest. Als Mitglied des Lenkungsausschusses und des Technischen Ausschusses der DMTF bietet HP Hard- und Software auf der Grundlage des DMI-Standards an.

Weitere Informationen über die Konfiguration der DMI-Software finden Sie in der Hilfdatei des *Intelligent Manageability Guide*.

## Wired for Management

Die Initiative *Wired for Management* von Intel hat das Ziel, die Kosten für Support und Administration von auf Intel Architekturen basierenden Systemen zu reduzieren, ohne dabei die Flexibilität oder Leistung zu beeinträchtigen. Die Richtlinien der *Wired for Management*-Initiative bieten einige grundlegende Bausteine, die HP für Intelligent Manageability nutzt, um eine standardisierte Verwaltung von Desktop-Inventar, einer Remote-Konfiguration des Systems, Wartung außerhalb der Geschäftszeiten und Energiesparfunktionen der nächsten Generation zu ermöglichen. HP beschränkt sich jedoch nicht auf diese Grundfunktionen. Intelligent Manageability wurde mit weiteren Funktionen ausgestattet, um eine umfassende Lösung für das Verwalten von vernetzten Computerumgebungen anzubieten.

*Wired for Management*-Technologien umfassen:

- Desktop Management Interface (DMI) 2.0
- Remote System Installation
- Remote Wakeup und Remote Shutdown
- ACPI-Ready Hardware
- SMBIOS
- PXE (Pre-boot Execution)-Unterstützung

## **Bestandsüberwachung und Sicherheit**

Die auf dem Computer vorinstallierten Compaq AssetControl-Funktionen stellen Ihnen wichtige Daten zur Bestandsüberwachung bereit, die über HP Insight Manager-Produkte und Management Solutions Partner-Produkte verwaltet werden können. Die nahtlose automatische Integration von AssetControl und diesen Produkten ermöglicht Ihnen die Auswahl des Management-Tools, das für Ihre Umgebung am besten geeignet ist, und die Nutzung Ihrer Investitionen in bestehende Tools.

HP Computer werden mit der erforderlichen Hardware und Firmware zur vollständigen Unterstützung des DMI 2.0 Standards ausgestattet.

Darüber hinaus bietet HP mehrere Lösungen zur Steuerung des Zugriffs auf wichtige Komponenten und Daten an. Sicherheitsfunktionen wie der Smart Cover Sensor und das Smart Cover Lock, die für bestimmte Modelle verfügbar sind, schützen gegen unberechtigten Zugriff auf interne Komponenten des Computers. Durch die Deaktivierung von parallelen und seriellen sowie USB-Ports oder durch die Deaktivierung der Startfähigkeit von Wechsellaufwerken können Sie wertvolle Datenbestände schützen. Memory Change- und Smart Cover Sensor-Warnmeldungen können automatisch an HP Insight Manager Produkte weitergeleitet werden, um darauf aufmerksam zu machen, dass sich jemand unerlaubten Zugang zu den internen Komponenten des Computers verschafft.



Der Smart Cover Sensor und das Smart Cover Lock stehen als Zusatzoptionen für ausgewählte Systeme zur Verfügung.

---

Verwenden Sie die folgenden Dienstprogramme zur Verwaltung der Sicherheitseinstellungen auf HP Computern.

- Lokal, mit Hilfe der *Computer Setup Utilities*. Weitere Informationen und Anleitungen zur Verwendung dieser Dienstprogramme finden Sie im *Computer Setup (F10) Utility Handbuch*, das mit dem Computer geliefert wurde.
- Remote, mit Hilfe von System Software Manager. Diese Software ermöglicht den sicheren, konsistenten Einsatz und die Steuerung von Sicherheitseinstellungen über ein einfaches Befehlszeilen-Dienstprogramm.

Die folgende Tabelle und die folgenden Abschnitte beziehen sich auf das lokale Management von Sicherheitsfunktionen des Computers über die Computer Setup Utilities (F10).

---

## Sicherheitsfunktionen – Übersicht

Funktion	Zweck	Einrichtung
Start-Schutz bei Wechsellaufwerken	Verhindert den Systemstart über Wechsellaufwerke.	Im Menü der <i>Computer Setup Utilities (F10)</i> .
Deaktivierung von seriellen, parallelen, USB- oder Infrarotschnittstellen	Verhindert die Datenübertragung über die serielle, parallele, USB (USB = Universal Serial Bus)- oder Infrarotschnittstelle.	Im Menü der <i>Computer Setup Utilities (F10)</i> .
Power-On Password (Systemstart-Kennwort)	Verhindert den Zugriff auf den Computer bis zur Eingabe des Kennworts. Dies kann sowohl für den ersten Start als auch für einen Neustart gelten.	Im Menü der <i>Computer Setup Utilities (F10)</i> .
Setup Password (Setup-Kennwort)	Der Computer kann erst dann (über die Computer Setup Utilities) neu konfiguriert werden, wenn das Setup-Kennwort eingegeben wird.	Im Menü der <i>Computer Setup Utilities (F10)</i> .

---

---

## Sicherheitsfunktionen – Übersicht (Fortsetzung)

Funktion	Zweck	Einrichtung
Network Server Mode (Netzwerk-Server-Modus)	Stellt für Computer, die als Server verwendet werden, hervorragende Sicherheitsfunktionen bereit.	Im Menü der Computer Setup Utilities (F10).
DriveLock	Verhindert unbefugten Zugriff auf die Daten bestimmter Festplatten. Diese Funktion ist nur bei einigen Modellen verfügbar.	Im Menü der Computer Setup Utilities (F10).
Smart Cover Sensor	Zeigt an, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Kann so eingestellt werden, dass das Setup-Kennwort für den Neustart des Computers angegeben werden muss, wenn die Gehäuseabdeckung oder die Seitenabdeckung entfernt wurde. Weitere Informationen finden Sie im <i>Hardware-Referenzhandbuch</i> auf der <i>Documentation Library</i> CD.	Im Menü der Computer Setup Utilities (F10).
Master Boot Record Security (Master Boot Record-Sicherheit)	Kann unbeabsichtigte oder böswillige Änderungen am Master Boot Record der aktuellen startfähigen Festplatte verhindern und stellt ein Mittel zur Wiederherstellung des letzten als gut befundenen MBRs dar.	Im Menü der Computer Setup Utilities (F10).

**Sicherheitsfunktionen – Übersicht (Fortsetzung)**

Funktion	Zweck	Einrichtung
Memory Change-Warnmeldungen	Erkennt, ob Speichermodule hinzugefügt, verschoben oder entfernt wurden und benachrichtigt den Benutzer sowie den Systemadministrator.	Informationen zur Aktivierung dieser Warnmeldungen finden Sie im Online-Handbuch <i>Intelligent Manageability</i> .
Eigentümerkennung	Zeigt beim Systemstart Informationen über den Eigentümer (geschützt durch das Setup-Kennwort) an, die vom Systemadministrator eingegeben wurden.	Im Menü der <i>Computer Setup Utilities (F10)</i> .
Diebstahlsicherung	Verhindert den Zugriff auf das Innere des Computers, damit keine Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden können. Kann auch dazu verwendet werden, den Computer an einem unbeweglichen Gegenstand zu befestigen, um ihn gegen Diebstahl zu sichern.	Bringen Sie eine Diebstahlsicherung an, um den Computer an einem unbeweglichen Gegenstand zu befestigen.
Ringschloss	Verhindert den Zugriff auf das Innere des Computers, damit keine Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden können.	Bringen Sie ein Ringschloss an, um zu verhindern, dass ungewollte Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden.



Weitere Informationen zu *Computer Setup* finden Sie im *Computer Setup (F10) Utility Handbuch*.

Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

## Kennwort-Schutz

Das Kennwort für den Systemstart verhindert eine unbefugte Verwendung des Computers, indem für den Zugriff auf Anwendungen oder Daten bei jedem Einschalten oder Neustart des Computers die Eingabe eines Kennwort verlangt wird. Das Setup-Kennwort verhindert insbesondere den unbefugten Zugriff auf *Computer Setup* und kann auch zur Übergehung des Kennworts für den Systemstart verwendet werden. Der Zugriff auf den Computer wird also gewährt, wenn bei der Eingabeaufforderung für das Kennwort für den Systemstart statt dessen das Setup-Kennwort eingegeben wird.

Ein Kennwort für das gesamte Netzwerk kann festgelegt werden, damit der Systemadministrator sich für Wartungsarbeiten bei allen Netzwerksystemen anmelden kann, ohne das Kennwort für den Systemstart zu kennen, selbst wenn dieses festgelegt wurde.

### Einrichten eines Setup-Kennworts über Computer Setup

Wenn ein Setup-Kennwort über *Computer Setup* eingerichtet wird, können Sie den Computer nur dann über Computer Setup Utility (F10) neu konfigurieren, wenn Sie das Kennwort eingeben.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung *F10 Setup* in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zugreifen zu können.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Setup Password** (Setup-Kennwort). Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes** (Änderungen speichern) und **Exit** (Schließen).

## Einrichten eines Kennworts beim Systemstart über Computer Setup

Die Einrichtung eines Kennworts für den Systemstart über *Computer Setup* verhindert den unbefugten Zugriff auf den Computer, wenn kein Kennwort eingegeben wird. Bei der Festlegung eines Kennworts für den Systemstart zeigt *Computer Setup* im Sicherheitsmenü Kennwoptionen an. Kennwoptionen sind *Network Server Mode* (Netzwerk-Servermodus) und *Password Prompt on Warm Boot* (Aufforderung zur Eingabe des Kennworts beim Warmstart).

Bei Deaktivierung von *Network Server Mode* (Netzwerk-Servermodus) muss das Kennwort jedes Mal eingegeben werden, wenn der Computer eingeschaltet und das Schlüsselsymbol auf dem Bildschirm angezeigt wird. Bei Aktivierung von *Password Prompt on Warm Boot* (Aufforderung zur Eingabe des Kennworts beim Warmstart) muss das Kennwort auch bei jedem Neustart eingegeben werden. Bei Aktivierung von *Network Server Mode* (Netzwerk-Servermodus) erscheint die Aufforderung zur Kennworteingabe nicht während des POST; sondern jede angeschlossene PS/2-Tastatur bleibt so lange gesperrt, bis der Benutzer das Kennwort für den Systemstart eingegeben hat.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung *F10 Setup* in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zugreifen zu können.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Power-On Password** (Systemstart-Kennwort). Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes** (Änderungen speichern) und **Exit** (Schließen).

## Eingeben eines Kennworts für den Systemstart

So geben Sie ein Kennwort für den Systemstart ein:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn das Schlüsselsymbol auf dem Bildschirm angezeigt wird, geben Sie Ihr aktuelles Kennwort ein, und drücken Sie die **Eingabetaste**.



Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

Wenn Sie das Kennwort falsch eingeben, erscheint ein durchgestrichenes Schlüsselsymbol. Versuchen Sie es noch einmal. Nach drei misslungenen Versuchen müssen Sie den Computer aus- und wieder einschalten, um fortfahren zu können.

## Eingeben eines Setup-Kennworts

Wenn für den Computer ein Setup-Kennwort eingerichtet wurde, werden Sie jedes Mal zur Eingabe dieses Kennworts aufgefordert, wenn Sie das Programm *Computer Setup* starten.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung *F10 = Setup* in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zugreifen zu können.

- 
3. Wenn das Schlüsselsymbol auf dem Bildschirm angezeigt wird, geben Sie das Setup-Kennwort ein, und drücken Sie die **Eingabetaste**.



Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

---

Wenn Sie das Kennwort falsch eingeben, erscheint ein durchgestrichenes Schlüsselsymbol. Versuchen Sie es noch einmal. Nach drei misslungenen Versuchen müssen Sie den Computer aus- und wieder einschalten, um fortfahren zu können.

## Ändern des Kennworts für den Systemstart oder des Setup-Kennworts

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**. Starten Sie das Programm *Computer Setup*, um das Setup-Kennwort zu ändern.
2. Wenn das Schlüsselsymbol angezeigt wird, geben Sie Ihr aktuelles Kennwort, einen Schrägstrich (/) oder ein anderes Begrenzungszeichen, Ihr neues Kennwort, einen weiteren Schrägstrich (/) oder ein anderes Begrenzungszeichen und ein zweites Mal Ihr neues Kennwort folgendermaßen ein:  
**aktuelles Kennwort/neues Kennwort/neues Kennwort**



Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

3. Drücken Sie die **Eingabetaste**.

Das neue Kennwort gilt ab dem nächsten Start des Computers.



Weitere Informationen zu Begrenzungszeichen finden Sie im Abschnitt *Begrenzungszeichen auf landesspezifischen Tastaturen* in diesem Kapitel. Das Kennwort für den Systemstart und das Setup-Kennwort können auch unter Verwendung der Sicherheitsfunktionen in *Computer Setup* geändert werden.

## Löschen des Kennworts für den Systemstart oder des Setup-Kennworts

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**. Starten Sie das Programm *Computer Setup*, um das Setup-Kennwort zu löschen.
2. Wenn das Schlüsselsymbol angezeigt wird, geben Sie Ihr aktuelles Kennwort und einen Schrägstrich (/) oder ein anderes Begrenzungszeichen ein (siehe unten): **aktueller Kennwort/**

### 3. Drücken Sie die **Eingabetaste.**



Weitere Informationen zu Begrenzungszeichen finden Sie unter *Begrenzungszeichen auf landesspezifischen Tastaturen*. Das Kennwort für den Systemstart und das Setup-Kennwort können auch unter Verwendung der Sicherheitsfunktionen in *Computer Setup* geändert werden.

---

## **Begrenzungszeichen auf landesspezifischen Tastaturen**

Jede Tastatur wurde an die landesspezifischen sprachlichen Besonderheiten angepasst. Die Syntax und die Tasten, die Sie zum Ändern oder Löschen Ihres Kennworts verwenden, hängen vom Tastaturlayout Ihres Computers ab.

### **Begrenzungszeichen auf landesspezifischen Tastaturen**

Arabisch	/	Griechisch	-	Russisch	/
Belgisch	=	Hebräisch	-	Slowakisch	-
BHKSJ*	-	Ungarisch	-	Spanisch	-
Brasilianisch	/	Italienisch	-	Schwedisch/ Finnisch	/
Chinesisch	/	Japanisch	/	Schweizerisch	-
Tschechisch	-	Koreanisch	/	Taiwanesisch	/
Dänisch	-	Latein- amerikanisch (Spanisch/ Portugiesisch)	-	Thailändisch	/
Französisch	!	Norwegisch	-	Türkisch	-
Kan. Französisch	é	Polnisch	-	Britisches Englisch	/
Deutsch	-	Portugiesisch	-	Amerikanisches Englisch	/

\*Bosnien-Herzegowina, Kroatien, Slowenien und Jugoslawien

## Löschen von Kennwörtern

Wenn Sie das Benutzerkennwort nicht mehr wissen, können Sie nicht mehr auf Ihren Computer zugreifen. Anleitungen zum Löschen von Kennwörtern finden Sie im *Fehlerbeseitigungs-Handbuch*.

## Network Server Mode (**Netzwerk-Server-Modus**)

Die Option *Network Server Mode* (Netzwerk-Server-Modus) bietet für Computer, die als Server verwendet werden, hervorragende Sicherheitsfunktionen. Sie steht nur zur Verfügung, wenn in *Computer Setup* ein Kennwort für den Systemstart festgelegt wurde. Bei Aktivierung von *Network Server Mode* (Netzwerk-Server-Modus) ist das Kennwort für den Systemstart zum Hochfahren der Festplatte nicht erforderlich, und an das System muss keine Tastatur angeschlossen sein. Wenn eine PS/2-Tastatur verwendet wird, bleibt diese solange gesperrt, bis der Benutzer das Kennwort für den Systemstart eingegeben hat. Eine USB-Tastatur kann standardmäßig weiterhin benutzt werden. Um einen Zugriff auf die USB-Tastatur nach dem Hochfahren des Systems zu verhindern, muss der USB-Anschluss über das Sicherheitsmenü von *Computer Setup* unter *Device Security* (Gerätesicherheit) ausgeblendet werden. In Verbindung mit der Option *After Power Loss power-on* (Inbetriebnahme nach Stromausfall) von *Computer Setup* ermöglicht *Network Server Mode* (Netzwerk-Server-Modus) es dem Server, nach einem Stromausfall automatisch ohne Benutzereingriff wieder hochzufahren. Wenn *Network Server Mode* (Netzwerk-Server-Modus) aktiviert ist, muss das Kennwort für den Systemstart eingegeben werden, um Wechselmedien (z. B. Disketten) oder externe Geräte (z. B. USB-Flash-Geräte) zu starten.

## DriveLock

*DriveLock* ist eine Sicherheitsfunktion, die den unbefugten Zugriff auf Daten bestimmter Festplatten verhindert. *DriveLock* wurde als Erweiterung von *Computer Setup* entwickelt. Diese Funktion steht nur bei einigen Systemen zur Verfügung, und zwar nur dann, wenn diese Systeme *DriveLock*-fähige Festplatten besitzen.

*DriveLock* ist für HP Kunden bestimmt, deren oberste Priorität Datenschutz ist. Für diese Kunden stehen die Kosten einer Festplatte und der Verlust der darauf gespeicherten Daten in keinem Verhältnis zu dem Schaden, der bei unberechtigtem Zugriff auf ihren Inhalt entstehen kann. Damit dieses hohe Sicherheitsniveau nicht zu allzu großen Problemen führt, wenn ein Kennwort vergessen wird, verwendet *DriveLock* ein Sicherheitssystem, das auf zwei Kennwörtern beruht. Dabei sollte ein Kennwort vom Systemadministrator festgelegt und verwendet werden, während das zweite normalerweise vom Benutzer erstellt und verwendet wird. Wenn beide Kennwörter vergessen werden, gibt es keine Möglichkeit mehr, um das Laufwerk zu entsperren. Deshalb ist die Verwendung von *DriveLock* am sichersten, wenn die auf der Festplatte enthaltenen Daten in ein Firmeninformationssystem repliziert oder regelmäßig gesichert werden.

Falls beide Kennwörter für *DriveLock* vergessen werden, bleibt der Zugriff auf die Festplatte für immer gesperrt. Dies mag für alle Benutzer, die nicht dem obigen Kundenprofil entsprechen, ein inakzeptables Risiko bedeuten. Dagegen bedeutet dies für Benutzer, die dem Profil entsprechen, im Hinblick auf die Art der auf der Festplatte gespeicherten Daten ein Risiko, das hingenommen werden kann.

## Verwenden von DriveLock

In *Computer Setup* ist *DriveLock* eine Option im Sicherheitsmenü. Dem Benutzer stehen Möglichkeiten zur Festlegung des Masterkennworts oder zur Aktivierung von *DriveLock* zur Verfügung. Zur Aktivierung von *DriveLock* muss ein Benutzerkennwort angegeben werden. Da die erste Konfiguration von *DriveLock* normalerweise vom Systemadministrator ausgeführt wird, sollte zuerst ein Masterkennwort festgelegt werden. HP befürwortet immer die Festlegung eines Masterkennworts durch den Administrator, unabhängig davon, ob er *DriveLock* aktivieren will oder ob es deaktiviert bleiben soll. Dadurch hat der Administrator die Möglichkeit, *DriveLock*-Einstellungen zu ändern, wenn das Laufwerk einmal gesperrt sein sollte. Ist das Masterkennwort einmal festgelegt, kann der Administrator *DriveLock* entweder aktivieren oder deaktiviert lassen.

Bei einer gesperrten Festplatte wird beim POST ein Kennwort zum Ent sperren abgefragt. Wenn ein Kennwort für den Systemstart festgelegt ist, das dem Benutzerkennwort für das Gerät entspricht, wird beim POST nicht erneut zur Eingabe des Kennworts aufgefordert. Andernfalls wird der Benutzer zur Eingabe eines *DriveLock*-Kennworts aufgefordert. Dabei kann entweder das Master- oder das Benutzerkennwort verwendet werden. Benutzern stehen zwei Versuche zur richtigen Kennworteingabe frei. Wird zweimal das falsche Kennwort eingegeben, wird POST fortgesetzt, es besteht aber weiterhin kein Zugriff auf Daten der Festplatte.

## Anwendungen von DriveLock

Am besten ist die *DriveLock*-Sicherheitsfunktion für eine Firmenumgebung geeignet, in der der Systemadministrator die Computer einiger Benutzer mit Multibay Festplattenlaufwerken ausstattet. Der Systemadministrator hat die Aufgabe, das Multibay Festplattenlaufwerk zu konfigurieren, das heißt unter anderem, auch das *DriveLock*-Masterkennwort festzulegen. Falls der Benutzer das Benutzerkennwort vergisst oder das Gerät an einen anderen Mitarbeiter weitergegeben wird, kann das Masterkennwort immer dazu verwendet werden, das Benutzerkennwort zurückzusetzen oder auf die Festplatte zuzugreifen.

HP empfiehlt Firmensystemadministratoren, die *DriveLock* aktivieren wollen, die Erstellung einer Firmenrichtlinie zur Einrichtung und Verwaltung von Masterkennwörtern. Dadurch soll vermieden werden, dass ein Mitarbeiter vor seinem Ausscheiden aus der Firma absichtlich oder unabsichtlich beide *DriveLock*-Kennwörter festlegt. In einem solchen Fall würde die Festplatte unbrauchbar und müsste ersetzt werden. Außerdem könnte es passieren, dass Systemadministratoren, die kein Masterkennwort festlegen, selbst eine gesperrte Festplatte vorfinden und dadurch keine Routineüberprüfungen auf nicht autorisierte Software, andere Bestandskontrollfunktionen und Supportaktivitäten mehr ausführen können.

Benutzern mit niedrigeren Sicherheitsanforderungen empfiehlt HP die Aktivierung von *DriveLock* nicht. Dazu zählen private Benutzer oder Benutzer, die auf ihrer Festplatte für gewöhnlich keine streng geheimen Daten aufbewahren. Für diese Benutzer ist der mögliche Verlust einer Festplatte aufgrund von zwei vergessenen Kennwörtern größer als der Wert, den *DriveLock* schützen soll. Der Zugriff auf *Computer Setup* und *DriveLock* kann durch das Setup-Kennwort eingeschränkt werden. Durch das Festlegen eines Setup-Kennworts, das nicht an Endbenutzer weitergegeben wird, können Systemadministratoren vermeiden, dass Benutzer *DriveLock* aktivieren.

## Smart Cover Sensor

Der Smart Cover Sensor (nur bei einigen Modellen), eine Kombination aus Hardware- und Softwaretechnologie, gibt eine Warnmeldung aus, wenn die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Es gibt drei Schutzstufen, die in der folgenden Tabelle beschrieben werden.

### Schutzstufen des Smart Cover Sensors

Stufe	Einstellung	Beschreibung
Stufe 0	Disabled (Deaktiviert)	Der Smart Cover Sensor ist deaktiviert (Standardeinstellung).
Stufe 1	Notify User (Benutzer benachrichtigen)	Wenn der Computer neu gestartet wird, wird auf dem Bildschirm eine Meldung darüber angezeigt, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde.
Stufe 2	Setup Password (Setup-Kennwort)	Wenn der Computer neu gestartet wird, wird auf dem Bildschirm eine Meldung darüber angezeigt, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Sie müssen das Setup-Kennwort eingeben, um fortfahren zu können.



Diese Einstellungen können mit Hilfe von *Computer Setup* geändert werden. Weitere Informationen zu *Computer Setup* finden Sie im *Computer Setup (F10) Utility Handbuch*.

## Einstellen der Schutzstufe für den Smart Cover Sensor

So stellen Sie eine Schutzstufe für den Smart Cover Sensor ein:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung *F10 Setup* in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zugreifen zu können.

---

3. Wählen Sie **Security** (Sicherheit) und anschließend **Smart Cover**. Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes** (Änderungen speichern) und **Exit** (Schließen).

## Smart Cover Lock

Das Smart Cover Lock ist eine über die Software gesteuerte Abdeckungsverriegelung, mit der einige HP Computermodelle ausgestattet sind. Sie verhindert den unbefugten Zugriff auf die inneren Komponenten des Computers. Die Computer werden mit deaktiviertem Smart Cover Lock geliefert.

---



**ACHTUNG:** Für die maximale Sicherheit der Abdeckungsverriegelung müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert den unbefugten Zugriff auf *Computer Setup*.

---



Das Smart Cover Lock ist als Zusatzoption für bestimmte Systeme erhältlich.

---

## Aktivieren des Smart Cover Locks

So aktivieren Sie die Sperrfunktion des Smart Cover Locks:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu.  
Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**.  
Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zugreifen zu können.

3. Wählen Sie **Security** (Sicherheit), dann **Smart Cover** und anschließend die Option **Locked** (Gesperrt).
4. Klicken Sie zum Beenden auf **File** (Datei) > **Save Changes** (Änderungen speichern) und **Exit** (Schließen).

## Entsperrnen des Smart Cover Locks

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung **F10 Setup** in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**.  
Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zugreifen zu können.

3. Wählen Sie **Security** (Sicherheit) > **Smart Cover > Unlocked** (Entsperrt).
4. Klicken Sie zum Beenden auf **File** (Datei) > **Save Changes** (Änderungen speichern) und **Exit** (Schließen).

## Verwenden des Smart Cover FailSafe-Schlüssels

Wenn das Smart Cover Lock aktiviert ist und Sie Ihr Benutzerkennwort nicht eingeben können, um die Sperre zu deaktivieren, brauchen Sie einen Smart Cover FailSafe-Schlüssel, um die Gehäuseabdeckung öffnen zu können. Sie brauchen den Schlüssel in den folgenden Fällen:

- Stromausfall
- Fehlgeschlagener Systemstart
- Ausfall einer PC-Komponente (z. B. Prozessor oder Netzteil)
- Kennwort vergessen



**ACHTUNG:** Der Smart Cover-FailSafe-Schlüssel ist ein spezielles Tool, das von HP angeboten wird. Bestellen Sie diesen Schlüssel am besten, bevor Sie ihn wirklich benötigen bei einem autorisierten Händler oder Servicepartner (Bestellnummer 166527-001 für den schraubenschlüsselartigen Schlüssel oder Bestellnummer 166527-002 für den schraubendreherartigen Schlüssel).

Führen Sie eines der folgenden Verfahren durch, um den FailSafe-Schlüssel zu erhalten:

- Wenden Sie sich an Ihren HP Partner oder Servicepartner.
- Lesen die Bestellinformationen unter <http://www.compaq.com> nach.
- Rufen Sie die in der Garantieerklärung genannte Rufnummer an.

Weitere Informationen zur Verwendung des Smart Cover FailSafe-Schlüssels finden Sie im *Hardware-Referenzhandbuch*.

## Master Boot Record Security (Master Boot Record-Sicherheit)

Der Master Boot Record (MBR) enthält Informationen, die für den erfolgreichen Start von einer Diskette aus und den Zugriff auf die auf der Diskette gespeicherten Daten erforderlich sind. Mit Hilfe von *Master Boot Record Security* können unbeabsichtigte oder böswillige Änderungen am MBR verhindert werden, die beispielsweise durch Viren oder die unkorrekte Verwendung von bestimmten Festplattendienstprogrammen verursacht werden. Sie haben außerdem die Möglichkeit, den letzten als gut befundenen MBR wiederherzustellen, wenn Sie beim Neustart des Systems Änderungen am MBR feststellen.

So aktivieren Sie die MBR-Sicherheit:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung *F10 Setup* in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zugreifen zu können.

3. Wählen Sie **Security** (Sicherheit) > **Master Boot Record Security** (Master Boot Record-Sicherheit) > **Enabled** (Aktiviert).
4. Wählen Sie **Security** (Sicherheit) > **Save Master Boot Record** (Master Boot Record speichern).
5. Klicken Sie zum Beenden auf **File** (Datei) > **Save Changes** (Änderungen speichern) und **Exit** (Schließen).

Wenn die MBR-Sicherheit aktiviert ist, verhindert das BIOS sämtliche Änderungen am MBR der aktuellen startfähigen Festplatte, solange in MS-DOS oder Windows der geschützte Modus aktiviert ist.



Die meisten Betriebssysteme steuern den Zugriff auf den MBR der aktuellen startfähigen Festplatte. Das BIOS kann keine Änderungen verhindern, die während der Ausführung des Betriebssystems erfolgen.

Bei jedem Einschalten oder Neustart des Computers vergleicht das BIOS den MBR der aktuellen startfähigen Festplatte mit dem zuvor gespeicherten MBR. Wenn Änderungen festgestellt werden und wenn es sich bei der aktuellen startfähigen Festplatte um dieselbe Festplatte handelt, von welcher der MBR zuvor gespeichert wurde, wird die folgende Meldung angezeigt:

1999 – Master Boot Record has changed (1999 – Master Boot Record wurde geändert).

Drücken Sie eine beliebige Taste, um *Computer Setup* zu starten und die MBR-Sicherheit zu konfigurieren.

Wenn Sie *Computer Setup* starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen startfähigen Festplatte
- Wiederherstellen des zuvor gespeicherten MBR oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

Wenn Änderungen festgestellt werden und wenn es sich bei der aktuellen startfähigen Festplatte **nicht** um dieselbe Festplatte handelt, von welcher der MBR zuvor gespeichert wurde, wird die folgende Meldung angezeigt:

2000 – Master Boot Record Hard Drive has changed  
(Master Boot Record der Festplatte wurde geändert).

Drücken Sie eine beliebige Taste, um *Computer Setup* zu starten und die MBR-Sicherheit zu konfigurieren.

Wenn Sie *Computer Setup* starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen startfähigen Festplatte oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

In dem unwahrscheinlichen Fall, dass der zuvor gespeicherte MBR beschädigt wurde, wird die folgende Meldung angezeigt:

1998 – Master Boot Record has been lost (1998 – Master Boot Record ist verloren gegangen).

Drücken Sie eine beliebige Taste, um *Computer Setup* zu starten und die MBR-Sicherheit zu konfigurieren.

Wenn Sie *Computer Setup* starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen startfähigen Festplatte oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

## Vor der Partitionierung oder Formatierung der aktuellen startfähigen Festplatte

Stellen Sie sicher, dass die MBR-Sicherheit deaktiviert ist, bevor Sie die Formatierung oder Partitionierung der aktuellen startfähigen Festplatte ändern. Einige Festplattendienstprogramme (wie z. B. FDISK und FORMAT) versuchen, den MBR zu aktualisieren. Wenn die MBR-Sicherheit aktiviert ist, während Sie die Partitionierung oder Formatierung der Festplatte ändern, erhalten Sie beim nächsten Start oder Neustart des Computers möglicherweise Fehlermeldungen vom Festplattendienstprogramm oder einen Warnhinweis von der MBR-Sicherheit. Führen Sie die folgenden Schritte durch, um die MBR-Sicherheit zu deaktivieren:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Wenn die Meldung *F10 Setup* in der unteren rechten Bildschirmecke angezeigt wird, drücken Sie die Taste **F10**. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.



Wenn Sie die Taste **F10** nicht drücken, während die Meldung angezeigt wird, müssen Sie den Computer erneut starten, um auf dieses Dienstprogramm zugreifen zu können.

3. Wählen Sie **Security** (Sicherheit) > **Master Boot Record Security** (Master Boot Record-Sicherheit) > **Enabled** (Aktiviert).
4. Klicken Sie zum Beenden auf **File** (Datei) > **Save Changes** (Änderungen speichern) und **Exit** (Schließen).

## Diebstahlsicherung

Die Anbringung einer Diebstahlsicherung ist auf der Rückseite des Computers möglich, so dass dieser an einem festen Gegenstand gesichert werden kann.

Anleitungen mit den entsprechenden Abbildungen finden Sie im *Hardware-Referenzhandbuch* auf der *Documentation Library CD*.

## Fingerprint Identification Technology

Die HP Fingerprint Identification Technology macht die Eingabe eines Benutzerkennwortes überflüssig, erhöht die Netzwerksicherheit, vereinfacht den Anmeldvgang und verringert die mit dem Management von Firmennetzwerken verbundenen Kosten. Wegen ihres erschwinglichen Preises ist sie nicht mehr nur High-Tech-Organisationen mit hohem Sicherheitsbedürfnis vorbehalten.



Die Unterstützung für die Fingerprint Identification Technology hängt von dem jeweiligen Modell ab.

---

Weitere Informationen finden Sie unter  
[http://www.compaq.com/products/quickspecs/10690\\_na/  
10690\\_na.html](http://www.compaq.com/products/quickspecs/10690_na/10690_na.html)

## Fehlermeldung und Fehlerbehebung

Die Funktionen zur Fehlermeldung und Fehlerbehebung kombinieren innovative Hardware- und Softwaretechnologien, um den Verlust wichtiger Daten zu verhindern und Ausfälle zu vermeiden.

Im Falle eines Fehlers gibt der Computer eine Warnmeldung aus, die den Fehler beschreibt und Vorsichtsmaßnahmen empfiehlt. Sie können sich dann den aktuellen Zustand des Systems über den HP Insight Management Agent anzeigen lassen. Wenn der Computer an ein Netzwerk angeschlossen ist, das von einem HP Insight Manager Produkt oder einem anderen Management-Produkt von Compaq Management Solutions Partners überwacht wird, sendet der Computer auch an die Netzwerk-Management-Anwendung eine Fehlermeldung.

## Drive Protection System

Das Drive Protection System (DPS) ist ein in die Festplattenlaufwerke bestimmter HP Computer integriertes Diagnose-Tool. Dieses Tool soll die Diagnostizierung von Problemen unterstützen, die zu einem ungerechtfertigten Festplattenaustausch führen könnten.

Jedes Festplattenlaufwerk wird vor dem Einbau in einen HP Computer unter Verwendung von DPS getestet, und wichtige Informationen werden permanent auf die Festplatte geschrieben. Die Testergebnisse werden bei jeder Ausführung von DPS auf das Festplattenlaufwerk geschrieben. Diese Informationen können Ihrem Compaq Servicepartner bei der Diagnose von Zuständen nützlich sein, die Sie zur Ausführung der DPS-Software veranlasst haben. Hinweise zur Verwendung von DPS finden Sie im *Fehlerbeseitigungs-Handbuch*.

## Ultra ATA Integritäts-Überwachung

Die Ultra ATA-Integritäts-Überwachung überwacht die Integrität der Daten während der Übertragung zwischen einer Ultra ATA-Festplatte und der Systemplatine. Wenn der Computer eine ungewöhnliche Anzahl von Übertragungsfehlern registriert, werden auf dem Bildschirm eine lokale Warnmeldung sowie empfohlene Maßnahmen angezeigt.

## **Überspannungstolerantes Netzteil**

Ein integriertes überspannungstolerantes Netzteil bietet eine größere Zuverlässigkeit, wenn der Computer einer unvorhergesehenen Überspannung ausgesetzt wird. Diese Stromversorgung wurde so konzipiert, dass sie eine Überspannung von bis zu 2000 V neutralisiert und Ausfälle sowie Datenverluste im System verhindert.

## **Thermosensor**

Der Thermosensor ist eine Hard- und Softwarefunktion zur Messung der Innentemperatur eines Computers. Diese Funktion zeigt eine Warnmeldung an, wenn der normale Temperaturbereich überschritten wird, so dass Sie Maßnahmen ergreifen können, bevor die internen Komponenten beschädigt werden oder Daten verloren gehen.

---

# Index

## A

- Abdeckungsverriegelung, Sicherheit,
  - Warnhinweis 32
- Abdeckungsverriegelung, Smart Cover Lock 32
- ActiveUpdate 8
- Aktivieren des Smart Cover Locks 33
- Altiris eXpress 4
- Altiris eXpress HP/Compaq Client Manager 6
- Altiris eXpress PC Transplant Pro 6
- Ändern des Kennworts 25
- AssetControl 17
- Aufrüsten des ROM 8

## B

- Begrenzungszeichen, Tabelle 26
- Benachrichtigung über Produktänderungen (PCN, Product Change Notification) 7
- Benutzerdefinierte Anpassung der Software 2
- Bestellen des FailSafe-Schlüssels 34
- Betriebssysteme, Wichtige Informationen 15

## C

- Cloning-Tools, Software 2
- Computer Setup Utilities 12

## D

- Datenintegrität 39
- Desktop Management Interface (DMI) 16
- Diagnose-Tool für Festplattenlaufwerke 39
- Diebstahlsicherung 38
- Diskette, Cloning 2
- DMI (Desktop Management Interface) 16
- Dual-State Netzschalter 13

## E

- Eingeben
  - Setup-Kennwort 24
  - Systemstart-Kennwort 23
- Einsatz-Tools, Software 2
- Einstellen
  - Setup-Kennwort 21, 24
  - Smart Cover Sensor 32
  - Systemstart-Kennwort 22
  - Timeout-Werte 14
- Energiesparfunktionen, Einstellungen 14
- Ent sperren des Smart Cover Locks 33
- Erste Konfiguration 2

## F

- FailSafe-Boot-Block-ROM 10
- FailSafe-Schlüssel
  - Bestellen 34
  - Warnhinweis 34
- Fehlermeldung 39
- Festplattenlaufwerke, Diagnose-Tool 39
- Fingerprint Identification Technology 38
- Formatieren der Festplatte, Wichtige Informationen 37

## I

- Innentemperatur des Computers 40
- Intelligent Manageability 16
- Internetadressen, Siehe Websites

## K

- Kennwort
  - Ändern 25
  - Löschen 25, 27
  - Setup 21, 24
  - Systemstart 22, 23

- Kennwortschutz 21  
Konfigurieren des Netzschalters 13
- L**  
Landesspezifische Tastaturen,  
Begrenzungszeichen 26  
Laufwerk, Schutz 39  
Löschen des Kennworts 25, 27
- M**  
Master Boot Record Security (Master Boot Record-Sicherheit), Einstellen 35
- N**  
Netzschatler  
Dual-State 13  
Konfigurieren 13  
Netzteil, Überspannungstolerant 40
- P**  
Partitionieren der Festplatte, Wichtige Informationen 37  
PCN, Product Change Notification  
(Benachrichtigung über Produktänderungen) 7  
Power Management 14
- R**  
Remote System Installation, Zugreifen auf 3  
Remote-ROM-Flash 9  
Remote-Setup 3  
ROM, Aufrüsten 8  
ROM, LED-Anzeigen auf der Tastatur, Tabelle 11  
ROM, Ungültig 9
- S**  
Schutz des Festplattenlaufwerks 39  
Schützen des ROM, Warnhinweis 8  
Setup, Erstmalig 2  
Setup, Replizieren 12
- Setup-Kennwort  
Ändern 25  
Eingeben 24  
Einstellen 21  
Löschen 25  
Sicherheit, Master Boot Record 35  
Sicherheitseinstellungen, Einrichten 17  
Sicherheitsfunktionen, Tabelle 18  
Smart Cover FailSafe-Schlüssel, Bestellen 34  
Smart Cover Lock  
Entsperrnen 33  
Sperrfunktion aktivieren 33  
Smart Cover Sensor  
Einstellen 32  
Schutzstufen 31  
Software  
Aktualisieren mehrerer Computer 7  
Altiris eXpress 4  
AssetControl 17  
Computer Setup Utilities 12  
Drive Protection System 39  
FailSafe-Boot-Block-ROM 10  
Fehlermeldung und Fehlerbehebung 39  
Integration 2  
Master Boot Record Security (Master Boot Record-Sicherheit) 35  
Power Management 14  
Remote System Installation 3  
Remote-ROM-Flash 9  
System Software Manager 7  
Wiederherstellung 2  
Sparen von Energie 14  
SSM (System Software Manager) 7  
Startfähige Festplatte, Wichtige Informationen 37  
Steuern des Computerzugriffs 17  
System Software Manager (SSM) 7  
System, Wiederherstellung 9

Systemstart-Kennwort

Ändern 25

Eingeben 23

Einstellen 22

Löschen 25

## T

Tastatur, LED-Anzeigen, ROM, Tabelle 11

Tastaturen, Begrenzungszeichen,  
Landesspezifisch 26

Temperatur, Innere Komponenten 40

Thermosensor 40

Timeout-Werte, Einstellen 14

## U

Überspannungstolerantes Netzteil 40

Ultra ATA Integritäts-Überwachung 39

Ungültiger ROM-Speicher 9

URLs (Websites). Siehe Websites

## V

Vorinstalliertes Software-Image 2

## W

Warnhinweise

Abdeckungsverriegelung, Sicherheit 32

FailSafe-Schlüssel 34

Schützen des ROM 8

Web-Adressen. Siehe Websites

Websites

[www.compaq.com](http://www.compaq.com) 8, 15, 34

[www.compaq.com/activeupdate](http://www.compaq.com/activeupdate) 8

[www.compaq.com/easydeploy](http://www.compaq.com/easydeploy) 5, 6, 9,  
12, 15

[www.compaq.com/im/ssmwp.html](http://www.compaq.com/im/ssmwp.html) 7, 8

[www.compaq.com/pcn](http://www.compaq.com/pcn) 7

[www.compaq.com/products/quickspecs/  
10690\\_na/10690\\_na.html](http://www.compaq.com/products/quickspecs/10690_na/10690_na.html) 38

[www.compaq.com/solutions/pcsolu](http://www.compaq.com/solutions/pcsolu)  
2

Wechseln von Betriebssystemen, Wichtige  
Informationen 15

Wiederherstellen des Systems 9

Wiederherstellung, Software 2

Wired for Management-Technologien 16

## Z

Zugriff auf Computer, Steuern 17

